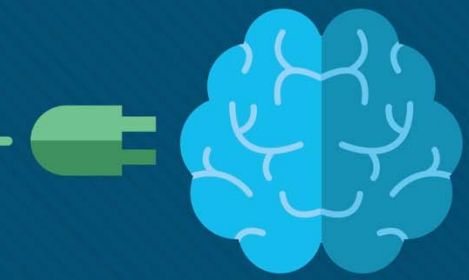
Hyrje ne sigurine e te dhenave

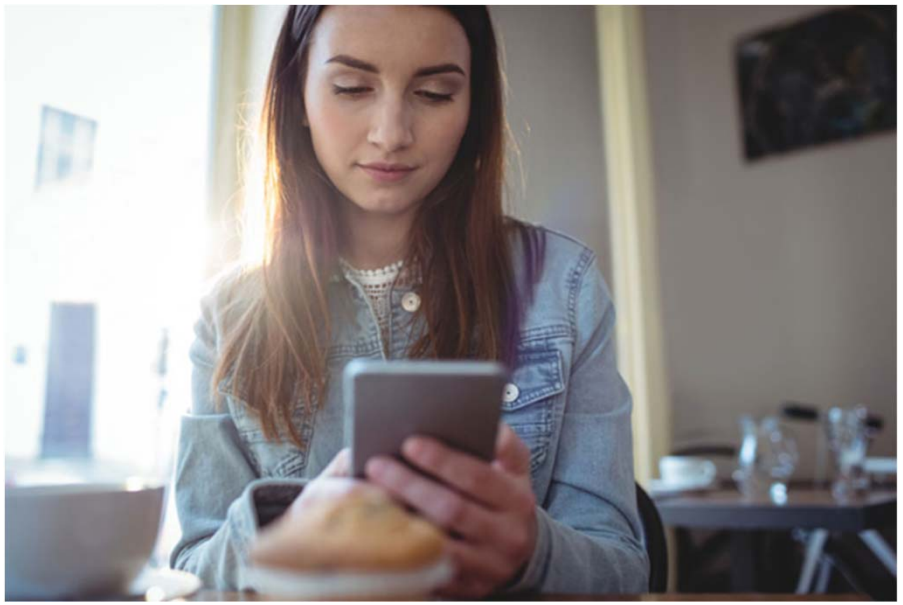


Objektivat e ligjëratës

- Rreziku
  - Shpjegoni pse rrjetet dhe të dhënat sulmohen.
  - Përshkruani karakteristikat e shembujve të incidenteve të sigurisë kibernetike.
  - Shpjegoni motivet e aktorëve të kërcënimit pas incidenteve specifike të sigurisë.
  - Shpjegoni ndikimin e mundshëm të sulmeve të sigurisë në rrjet.
- Luftëtarët në Luftën Kundër Krimit Kibernetik
  - Shpjegoni se si të përgatiteni për një karrierë në operacionet e sigurisë kibernetike.
  - Shpjegoni misionin e qendrës së operacioneve të sigurisë (SOC).
  - Përshkruani burimet në dispozicion për t'u përgatitur për një karrierë në operacionet e sigurisë kibernetike.

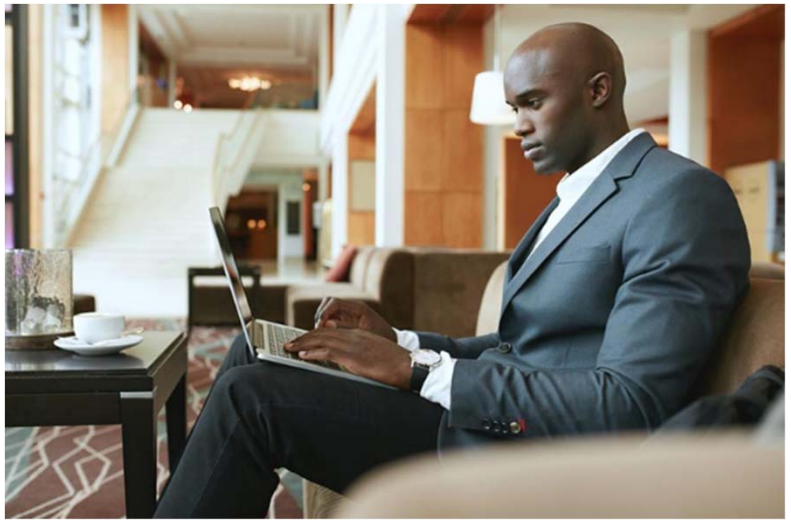
Tregime të Luftës Kibernetike
Hijacked People

- Një haker ngriti një hotspot të hapur "mashtrues" që paraqet si një rrjet wireless legjitim.
- Një klient hyri në faqen e internetit të bankës së saj.
- Hakeri kyqet në seancën e saj.
- Hakeri fiton qasje në llogaritë e saj bankare.



Tregime të Luftës Kibernetike
Kompanitë me Ransomware

- Një punonjës merr një email nga CEO i tij, që përmban një PDF të bashkangjitur.
- Ransomware është instaluar në kompjuterin e punonjësit.
- Ransomware grumbullon dhe krijon të dhënat e korporatave.
- Sulmuesit mbajnë të dhënat e kompanisë për shpërblim derisa ato të paguhen.



Tregime të Luftës Kibernetike
Kombet e synuara

- Stuxnet Worm
  - Infiltruar në sistemet operative të Windows.
  - Qëllimi i aplikacionit është Hapi 7 që kontrollon kontrollorët logjikë të programueshëm (PLC) për të dëmtuar centrifugat në objektet bërthamore.
  - Transmetohet nga disqet USB të infektuara në PLC dhe përfundimisht dëmtojnë shumë cetrifuga.

Sulmuesit Amatorë

- Njohur si kiddies script.
- Kanë pak ose aspak aftësi.
- Përdorni mjete ekzistuese ose udhëzime të gjetura në internet për të nisur sulme.

Sulmuesit
Hacktivists

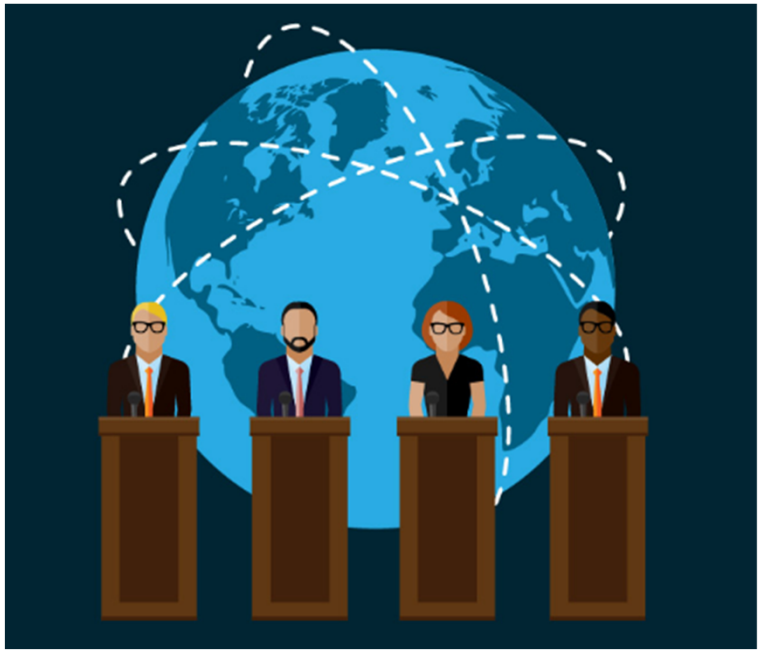
- Protesta kundër organizatave ose qeverive
  - Shkruajnë artikuj dhe publikojnë video.
  - Rrjedhin Informacione koenfidenciale në publik
  - Ndalojnë shërbimet e webit përmes sulmeve DDoS.

Sulmuesit
Përfitimi financiar

- Shumë aktivitete të piraterisë motivohen nga përfitimi financiar.
- Kriminelët kibernetikë duan të gjenerojnë të hyra përmes këtyre aktiviteteve
- Sulmojnë llogari bankare
- Të dhëna Personale
- Çdo gjë tjetër që mund të aplikohet me qëllim të përfitimit

Sulmuesit
Sekretet e Tregtisë dhe Politikat Globale

- Shtetet janë gjithashtu të interesuara në përdorimin e hapësirës kibernetike
  - Të sulmojnë vendet e tjera
  - Ndërhyrja në politikën e brendshme
  - Spiunazh industrial
  - Të përfitojnë përparësi të rëndësishme në tregtinë ndërkombëtare

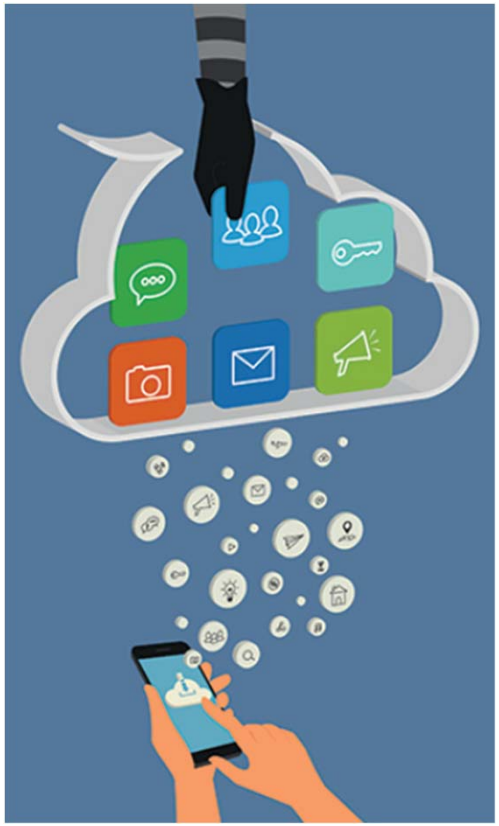


Sulmuesit
Sa i sigurt është Interneti I Gjërave (Internet of Things)

- Interneti i Gjërave (IoT)
- Ndërlidh gjërat për të përmirësuar cilësinë e jetës.
  - Shembull: fitness trackers
- Sa të sigurta janë këto pajisje?
  - Firmware
  - Gabimet e sigurisë
  - Përditësimi përmes patch
  - Sulmi DDoS kundër ofruesit të emrave të domain-it
- Kompromentimi I Webcams, DVR, routers, dhe pajisjet e tjera

Ndikimi i kërcënimeve
PII dhe PHI

- Informacioni personal i identifikueshëm (PII) është çdo informacion që mund të përdoret për identifikimin pozitiv të një individi.
- Shembujt e PII përfshijnë: emrin, numrin e ID, datën e lindjes, numrat e kartës së kreditit, numrat e llogarisë bankare, ID-të e lëshuara nga qeveria, adresën (rrugë, email, numrat e telefonit)
  - Këto infomacione shiten në tregun e zi apo rrjetin e errët.
  - Hackerët mund të krijojnë llogari të falsifikuara, si kartat e kreditit
- Informacioni Personal Shëndetësor:
  - Krijon dhe mirëmban të dhënat elektronike mjekësore (EMRs)
  - Rregulluar nga Akti i Transportueshmërisë dhe Përgjegjshmërisë së Sigurimeve Shëndetësore (HIPAA)

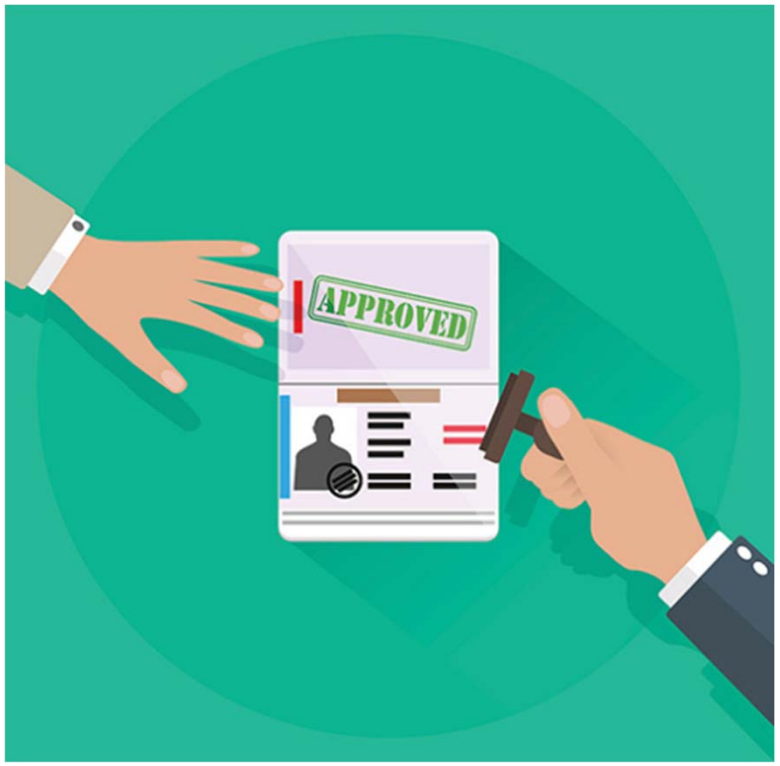


Ndikimi i kërcënimeve
Humbë Përparësinë Konkuruese

- Mund të rezultojë në avantazh konkurrues të humbur.
  - Spiunazhi i Korporatës në hapësirën kibernetike.
  - Humbja e besimit që vjen kur një kompani nuk është në gjendje të mbrojë të dhënat personale të klientëve të saj.

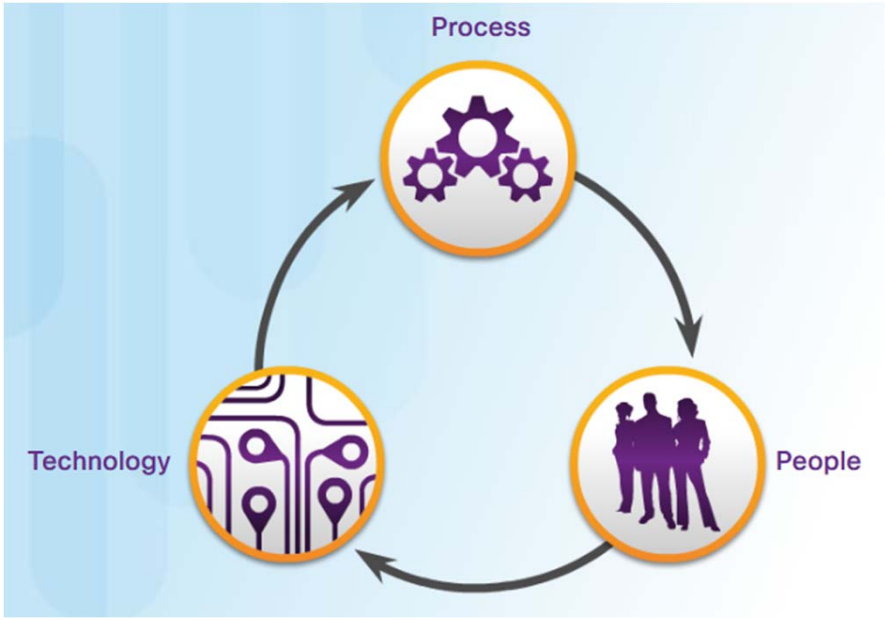
Ndikimi i kërcënimeve
Siguria Politike dhe Kombetare

- Në vitin 2016, një haker publikoi PII të 20,000 punonjësve të FBI-së së SHBA-së dhe 9,000 punonjës të SHS-së së SHBA.
- Stuxnet krim ishte projektuar për të penguar përparimin e Iranit në pasurimin e uraniumit
- Cyberwarfare është një mundësi serioze.
- Interneti është bërë thelbësor si një medium për aktivitetet tregtare dhe financiare.
- Përçarja mund të shkatërrojë ekonominë e një kombi dhe sigurinë e qytetarëve të saj.



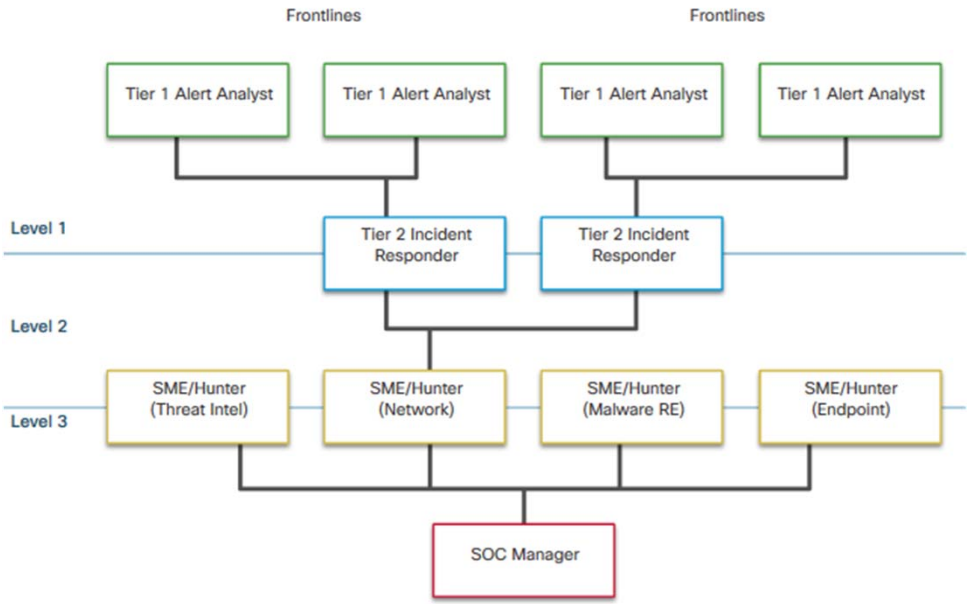
Qendra e Operacioneve të Sigurisë Moderne
Elementet e një SOC

- Qendrat e Operacioneve të Sigurisë (SOCs) ofrojnë një gamë të gjerë shërbimesh:
  - Monitorim
  - Udhëheqje
  - Zgjidhjet gjithëpërfshirëse të kërcënimeve
- SOC-të mund të jenë:
  - Në shtëpi, në pronësi si dhe duke operuar nga një biznes.
- Elementet mund të kontraktohen nga shitësit e sigurisë.
- Elementet kryesore të një SOC janë:
  - njerëz
  - proceset
  - teknologji



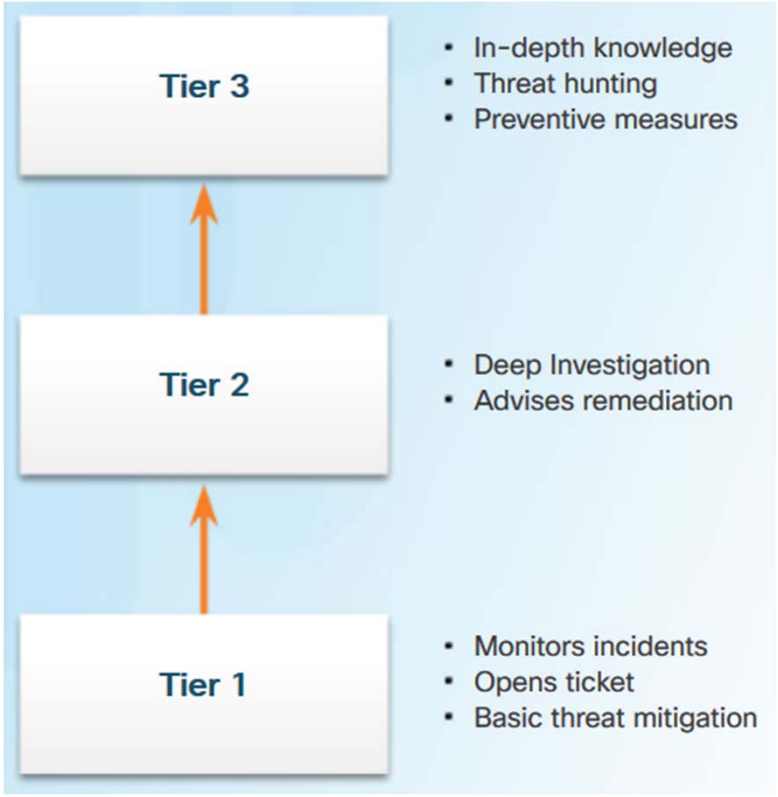
Qendra e Operacioneve të Sigurisë Moderne
Njerëzit në KOS

- Instituti SANS (www.sans.org) klasifikon rolin që njerëzit luajnë në një SOC në katër nivele :
  - **Analisti i Alertit në nivelin 1**
  - **Reaguesi i Incidentit në nivelin 2**
  - **Eksperti i lëndës (SME) / Hunter nënivelin 3**
  - **Menaxheri i SOC**



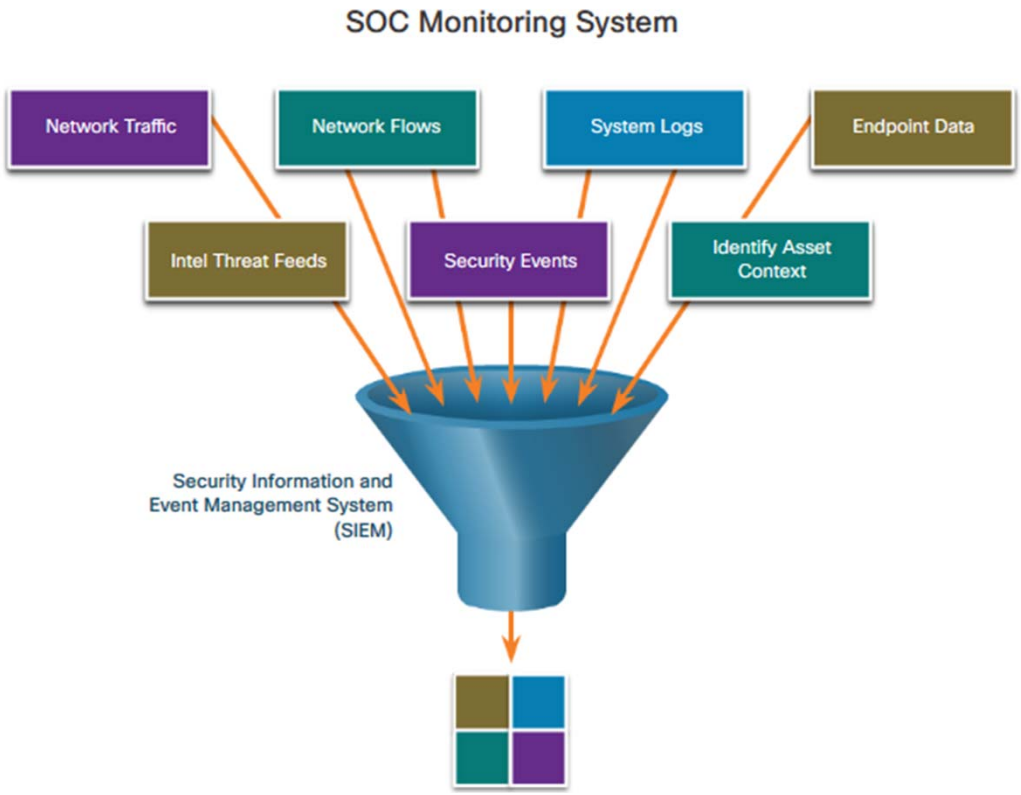
Qendra e Operacioneve të Sigurisë Moderne
Procesi në SOC

- Analisti i Alert - Niveli 1 fillon me monitorimin e rreshtave të alarmit të sigurisë.
- Analisti Alert – Niveli 1 verifikon nëse një alarm i shkaktuar në softuerin e biletave paraqet një incident të vërtetë sigurie.
- Incidenti mund të përcillet tek hetuesit, ose të zgjidhet si një alarm i rremë.



Qendra e Operacioneve të Sigurisë Moderne
Teknologjitë në SOC

- Sistemet e Informacionit të Sigurisë dhe Menaxhimit të Ngjarjeve (SIEM)
- Mbledhë dhe filtron të dhëna.
- Zbulon dhe klasifikon kërcënimet.
- Analizon dhe heton kërcënimet.
- Zbaton masat parandaluese.
- Adreson kërcënimet e ardhshme.



Qendra e Operacioneve të Sigurisë Moderne
Ndërmarrja dhe Siguria e Menaxhuar

- Organizatat mund të implementojnë një mekanizëm të nivelit SOC.
- SOC mund të jetë:
  - Një zgjidhje e plotë në shtëpi
  - Jepen të paktën një pjesë të operacioneve të SOC tek një ofrues i zgjidhjeve të sigurisë.

Qendra e Operacioneve të Sigurisë Moderne
Siguria kundrejt Disponueshmërisë

- Shumica e rrjeteve të ndërmarrjeve duhet të jenë të hapura dhe activi në çdo kohë.
- Uptime i preferuar shpesh matet në numrin e minutave të sistemit joaktiv në një vit. Një system mund të konsiderohet aktiv deri në 99.999% e kohës në se gjatë një viti ka pasur defente jo më shumë se 5 minuta e 26 sekonda.
- Ekziston një hapësirë e padefinuar nëmes të sigurisë së fortë dhe funksioneve të lejuara të biznesit.

Availability %	Downtime
99.8%	17.52 hours
99.9% (" three nines")	8.76 hours
99.99% (" four nines")	52.56 minutes
99.999% (" five nines")	5.256 minutes
99.9999% (" six nines")	31.5 seconds
99.99999% (" seven nines")	3.15 seconds

Përmbledhje

- Një rrjet "mashtrues" publik mund të përdoret për të fituar akses në të dhënat personale.
- Punonjësit e një kompanie mund të shkarkojnë ransomware pa dashje që mund të fillojnë procesin e grumbullimit dhe të kodimit të të dhënave të korporatës.
- Njohuritë e sofistikuara, worms Stuxnet, janë një shembull se si kombet mund të synojnë të ndikojnë në infrastrukturën e prekshme të vendit.
- Amateurs shkaktojnë dëme duke përdorur mjete të thjeshta të gjetura në internet.
- Hacktivistët janë hakerat me përvojë që punojnë për shkaqe të mira ose për qëllime të dëmshme.
- Shumë hakerë po kërkojnë vetëm fitime financiare duke vjedhur të holla në mënyrë elektronike, ose duke vjedhur sekretet tregtare të korporatave ose kombeve dhe duke shitur këtë informacion.
- Mbrojtja e një kombi kundër cyberespionage dhe cyberwarfare vazhdon të jetë një prioritet.
- Jini të vetëdijshëm për pasiguritë në Internetin e Gjërat.
- PII qëndron për informacion personalisht të identifikueshëm. ISH është informacion personal shëndetësor. Si PII dhe IPH mund të vidhen dhe përdoren për të fituar qasje në informata private.

Përmbledhje

- Humbja e përparësisë konkurruese mund të vijë nga humbja e besimit nëse një kompani nuk mund të mbrojë PII të klientëve të saj.
- Siguria kombëtare mund të ndërpritet nga hakerat. Krimb Stuxnet është një shembull.
- Elementet kryesore të një SOC janë njerëz, procese dhe teknologji.
- Qendrat e Operacioneve të Sigurisë punojnë për të luftuar krimin kibernetik.
- Njerëzit në një SOC janë Analistët e Grupit 1 (për të cilat është zhvilluar ky kurs), Tier 2 Incident Responders, Tier 3 SME / Gjuetarët dhe Menaxheri i KOS.
- Një analist i nivelit 1 monitoron rradhët e alarmit të sigurisë. Analisti i Grupit 1 mund të duhet të verifikojë se një alarm përfaqëson një incident të vërtetë sigurie. Kur të vërtetohet, incidenti mund të përcillet tek hetuesit, ose të zgjidhet si një alarm i rremë.
- Sistemet SIEM përdoren për grumbullimin dhe filtrimin e të dhënave, zbulimin dhe klasifikimin e kërcënimeve, analizimin dhe hetimin e kërcënimeve, zbatimin e masave parandaluese dhe adresimin e kërcënimeve në të ardhmen.

Përmbledhje

- Sllajdet punuar nga Blerton Abazi